The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:

06/20/2016

SUBJECT:

Multiple Vulnerabilities in Apache Struts Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered for Apache Software Foundation Struts version 2. Apache Struts is an open source framework used for building Java web applications. Successful exploitation of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Apache Struts versions 2.0.0 to 2.3.28.1

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: **N/A**

TECHNICAL SUMMARY

Multiple vulnerabilities have been discovered in Apache Struts, the most severe of which could allow for remote code execution. An attacker can exploit this issue by sending a specially crafted attribute data to execute remote code. The details of these vulnerabilities are as follows:

- A Remote Code Execution vulnerability exists within the Apache Struts framework because it performs double OGNL evaluation of attribute values assigned to certain tags (CVE-2016-0785).
- A Cross-Site Request Forgery vulnerability exists in Apache Struts because it fails to validate bypass tokens properly (CVE-2016-4430).
- Multiple Security Bypass vulnerabilities exist in Apache Struts which result in the ability to perform unauthorized actions (CVE-2016-4431, CVE-2016-4433, CVE-2016-4436).
- A Remote Code Execution vulnerability exists when using the REST plugin which could allow for arbitrary code execution of server code (CVE-2016-4438).

- A Denial of Service vulnerability exists in Apache Struts due to how the URLvalidator function improperly handles supplied input (CVE-2016-4465).

Successful exploitation of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to one of the non-impacted versions of Adobe Struts (2.3.29 or 2.5.1), or follow the mitigation identified in the referenced Apache resources below after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying the patch.
- Frequently validate type and content of uploaded data.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Apache:

https://struts.apache.org/docs/s2-035.html
https://struts.apache.org/docs/s2-036.html
https://struts.apache.org/docs/s2-037.html
https://struts.apache.org/docs/s2-038.html
https://struts.apache.org/docs/s2-039.html
https://struts.apache.org/docs/s2-040.html
https://struts.apache.org/docs/s2-041.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0785
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4430
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4431
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4433
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4436
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4438
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4465